PORTAL
USPTO

Search: ⦿ The ACM Digital Library ○ The Guide

SEARCH

THE ACM DIGITAL LIBRARY

⚡ Feedback

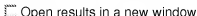(differential power analysis) and (differential and power and analysis and first and rounds)

Found 351 of 2,739

Terms used:
differential power analysis differential power analysis first rounds

Sort results by [relevance ▾]

📋 Save results to a Binder

Refine these results wi
Try this search in The /

Display results [expanded form ▾]

☐ Open results in a new window

Results 1 - 20 of 351   Result page: 1 2 3 4 5 6 7 8 9 10 next >>

1 Effective thread management on network processors with compiler analysis
Xiaotong Zhuang, Santosh Pande
June 2006 LCTES '06: Proceedings of the 2006 ACM SIGPLAN/SIGBED conference on Language,
          compilers, and tool support for embedded systems
Publisher: ACM

Full text available: 📄 pdf(466.13 KB)   Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 62, Citation Count: 0

   Mapping packet processing tasks on network processor micro-engines involves complex tradeoff
   that relating to maximizing parallelism and pipelining. Due to an increase in the size of the code
   store and complexity of the application requirements, network ...

   Keywords: CPU scheduling, compiler optimizations, network processors, real-time scheduling

2 Modeling and analysis of dynamic coscheduling in parallel and distributed environments
Mark S. Squillante, Yanyong Zhang, Anand Sivasubramaniam, Natarajan Gautam, Hubertus Franke
Jose Moreira
June 2002 ACM SIGMETRICS Performance Evaluation Review, Volume 30 Issue 1
Publisher: ACM

Full text available: 📄 pdf(257.68 KB)   Additional Information: full citation, abstract, references, cited by

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 54, Citation Count: 5

   Scheduling in large-scale parallel systems has been and continues to be an important and
   challenging research problem. Several key factors, including the increasing use of off-the-shelf
   clusters of workstations to build such parallel systems, have resulted ...

3 A 9.6 kb/s CMOS FSK modem for data transmission through power lines
Walter J. Lancioni, Pablo A. Petrashin, Luis E. Toledo, Carlos F. Dualibe
September 2007 SBCCI '07: Proceedings of the 20th annual conference on Integrated circuits and
              systems design
Publisher: ACM

Full text available: 📄 pdf(529.11 KB)   Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 137, Citation Count: 0

The design and test of a mixed-signal 9.6Kb/s FSK transmitter-receiver is presented. It is aimed for digital communications through the domiciliary power lines as needed by a networked electri power management and measuring system wherein the circuit ...

Keywords: analog CMOS, power line transceiver, switched capacitor amplifier

4   The equalizing impact of a group support system on status differentials
Bernard C. Y. Tan, Kwok-kee Wei, Richard T. Watson
January 1999 ACM Transactions on Information Systems (TOIS),   Volume 17 Issue 1
Publisher: ACM
Full text available: pdf(138.22 KB)   Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 9,   Downloads (12 Months): 50,   Citation Count: 2

This study investigates the impact of the electronic communication capability of a group support system (GSS) on status differentials in small groups. A laboratory experiment was used to answ the research questions. Three support levels were studied: ...

Keywords: electronic communication, group support systems, status differentials, task type

5   Design of secure cryptography against the threat of power-attacks in DSP-embedded processors
Catherine H. Gebotys
February 2004 ACM Transactions on Embedded Computing Systems (TECS),   Volume 3 Issue 1
Publisher: ACM
Full text available: pdf(214.56 KB)   Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 13,   Downloads (12 Months): 132,   Citation Count: 3

Embedded wireless devices require secure high-performance cryptography in addition to low-co: and low-energy dissipation. This paper presents for the first time a design methodology for security on a VLIW complex DSP-embedded processor core. Elliptic ...

Keywords: VLIW

6   Efficient and passive modeling of transmission lines by using differential quadrature metho
Q. Xu, P. Mazumder
March 2001 DATE '01: Proceedings of the conference on Design, automation and test in Europe
Publisher: IEEE Press
Full text available: pdf(171.50 KB)   Additional Information: full citation, references, index terms

Bibliometrics: Downloads (6 Weeks): 0,   Downloads (12 Months): 22,   Citation Count: 0

7   Bibliography on Numerical Analysis
Alston S. Householder
April 1956 Journal of the ACM (JACM),   Volume 3 Issue 2
Publisher: ACM
Full text available: pdf(1.12 MB)   Additional Information: full citation, references, index terms

Bibliometrics: Downloads (6 Weeks): 6,   Downloads (12 Months): 65,   Citation Count: 0

8 Approximate fairness through differential dropping
   Rong Pan, Lee Breslau, Balaji Prabhakar, Scott Shenker
   April 2003 ACM SIGCOMM Computer Communication Review, Volume 33 Issue 2
   Publisher: ACM
   Full text available: 🗎 pdf(2.07 MB)   Additional Information: full citation, abstract, references, cited by

   Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 63, Citation Count: 4
      Many researchers have argued that the Internet architecture would be more robust and more
      accommodating of heterogeneity if routers allocated bandwidth fairly. However, most of the
      mechanisms proposed to accomplish this, such as Fair Queueing [16, 6] ...

9 Analysis of benchmark characteristics and benchmark performance prediction
   Rafael H. Saavedra, Alan J. Smith
   November 1996 ACM Transactions on Computer Systems (TOCS), Volume 14 Issue 4
   Publisher: ACM
   Full text available: 🗎 pdf(1.02 MB)   Additional Information: full citation, abstract, references, cited by, index terms
                                                                  review

   Bibliometrics: Downloads (6 Weeks): 32, Downloads (12 Months): 202, Citation Count: 16
      Standard benchmarking provides to run-times for given programs on given machines, but fails t
      provide insight as to why those results were obtained (either in terms of machine or program
      characteristics) and fails to provide run-times for that program ...

      Keywords: abstract machine performance model, benchmark analysis, execution time predictic
      microbenchmarking

10 Battery power-aware encryption
   R. Chandramouli, S. Bapatla, K. P. Subbalakshmi, R. N. Uma
   May 2006 ACM Transactions on Information and System Security (TISSEC), Volume 9 Issue 2
   Publisher: ACM
   Full text available: 🗎 pdf(454.71 KB)   Additional Information: full citation, abstract, references, index terms

   Bibliometrics: Downloads (6 Weeks): 29, Downloads (12 Months): 209, Citation Count: 0
      Minimizing power consumption is crucial in battery power-limited secure wireless mobile networ
      In this paper, we (a) introduce a hardware/software set-up to measure the battery power
      consumption of encryption algorithms through real-life experimentation, ...

      Keywords: Low-power encryption, optimization, profiling

11 A Power-Aware Run-Time System for High-Performance Computing
   Chung-hsing Hsu, Wu-chun Feng
   November 2005 SC '05: Proceedings of the 2005 ACM/IEEE conference on Supercomputing
   Publisher: IEEE Computer Society
   Full text available: 🗎 pdf(566.46 KB)   Additional Information: full citation, abstract, references, cited by, index terms

   Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 81, Citation Count: 3
      For decades, the high-performance computing (HPC) community has focused on performance,
      where performance is defined as speed. To achieve better performance per compute node,
      microprocessor vendors have not only doubled the number of transistors (and ...

12 A fast decoupling capacitor budgeting algorithm for robust on-chip power delivery
Jingjing Fu, Zuying Luo, Xianlong Hong, Yici Cai, Sheldon X.-D. Tan, Zhu Pan
January 2004 ASP-DAC '04: Proceedings of the 2004 conference on Asia South Pacific design
        automation: electronic design and solution fair
Publisher: IEEE Press
Full text available: 📄 pdf(206.84 KB) 🔗 Publisher Site   Additional Information: full citation, abstract, references, cited by

Bibliometrics: Downloads (6 Weeks): 2,   Downloads (12 Months): 20,   Citation Count: 7
    In this paper, we present an efficient method to budget on-chip decoupling capacitors (decaps)
    optimize power delivery networks in an area efficient way. Our algorithm is based on an efficien
    gradient-based non-linear programming method for searching ...

13 Large-Scale First-Principles Molecular Dynamics simulations on the BlueGene/L Platform
   using the Qbox code
Francois Gygi, Robert K. Yates, Juergen Lorenz, Erik W. Draeger, Franz Franchetti, Christoph W.
Ueberhuber, Bronis R. de Supinski, Stefan Kral, John A. Gunnels, James C. Sexton
November 2005 SC '05: Proceedings of the 2005 ACM/IEEE conference on Supercomputing
Publisher: IEEE Computer Society
Full text available: 📄 pdf(347.84 KB)   Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 6,   Downloads (12 Months): 32,   Citation Count: 4
    We demonstrate that the Qbox code supports unprecedented large-scale First-Principles Molecul
    Dynamics (FPMD) applications on the BlueGene/L supercomputer. Qbox is an FPMD
    implementation specifically designed for large-scale parallel platforms such ...

    Keywords: Electronic structure. Molecular Dynamics. Ab initio simulations. First-principles
    simulations. Parallel computing. BlueGene/L.

14 Mobile power management for wireless communication networks
John M. Rulnick, Nicholas Bambos
March 1997 Wireless Networks,   Volume 3 Issue 1
Publisher: Kluwer Academic Publishers
Full text available: 📄 pdf(274.39 KB)   Additional Information: full citation, abstract, references, cited by, index terms
                                                            review
Bibliometrics: Downloads (6 Weeks): 14,   Downloads (12 Months): 120,   Citation Count: 20
    For fixed quality-of-service constraints and varying channel interference, how should a mobile
    node in a wireless network adjust its transmitter power so that energy consumption is minimize
    Several transmission schemes are considered, and optimal solutions ...

15 Adaptive multi-domain thermal modeling and analysis for integrated circuit synthesis and
   design
Yonghong Yang, Changyun Zhu, Zhenyu (Peter) Gu, Li Shang, Robert P. Dick
November 2006 ICCAD '06: Proceedings of the 2006 IEEE/ACM international conference on
        Computer-aided design
Publisher: ACM
Full text available: 📄 pdf(358.70 KB)   Additional Information: full citation, abstract, references, index terms

Chip-package thermal analysis is necessary for the design and synthesis of reliable, high-performance, low-power, compact integrated circuits (ICs). Many methods of IC thermal analysi suffer performance or accuracy problems that prevent use in IC synthesis ...

16 Power Attack Resistant Cryptosystem Design: A Dynamic Voltage and Frequency Switchin Approach
Shengqi Yang, Wayne Wolf, N. Vijaykrishnan, D. N. Serpanos, Yuan Xie
March 2005 DATE '05: Proceedings of the conference on Design, Automation and Test in Europe - Volume 3,   Volume 3
Publisher: IEEE Computer Society
Full text available: 📄 pdf(291.82 KB)   Additional Information: full citation, abstract, references, index terms

A novel power attack resistant cryptosystem is presented in this paper. Security in digital computing and communication is becoming increasingly important. Design techniques that can protect cryptosystems from leaking information have been studied by ...

17 The power of explicit congestion notification
Aleksandar Kuzmanovic
August 2005 SIGCOMM '05: Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications
Publisher: ACM
Full text available: 📄 pdf(251.91 KB)   Additional Information: full citation, abstract, references, index terms

Despite the fact that Explicit Congestion Notification (ECN) demonstrated a clear potential to substantially improve network performance, recent network measurements reveal an extremely poor *usage* of this option in today's Internet. In this paper, ...

Keywords: active queue management, congestion control, explicit congestion notification

18 An overview of side channel analysis attacks
Thanh-Ha Le, Cécile Canovas, Jessy Clédière
March 2008 ASIACCS '08: Proceedings of the 2008 ACM symposium on Information, computer and communications security
Publisher: ACM
Full text available: 📄 pdf(483.77 KB)   Additional Information: full citation, abstract, references, index terms

During the last ten years, power analysis attacks have been widely developed under many form They analyze the relation between the power consumption or electromagnetic radiation of a cryptographic device and the handled data during cryptographic operations. ...

Keywords: CPA, DEMA, DPA, side channel attacks, stochastic model, template attack

19 Performance analysis of a rate-based feedback control scheme
Lalita A. Kulkarni, San-qi Li

December 1998 IEEE/ ACM Transactions on Networking (TON), Volume 6 Issue 6
Publisher: IEEE Press
Full text available: pdf(419.31 KB)   Additional Information: full citation, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 25, Citation Count: 1

   Keywords: feedback control, numerical analysis, stochastic modeling, transient performance

20 Effective thread management on network processors with compiler analysis
    Xiaotong Zhuang, Santosh Pande
    July 2006   ACM SIGPLAN Notices, Volume 41 Issue 7
    Publisher: ACM
Full text available: pdf(466.13 KB)   Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 62, Citation Count: 0

    Mapping packet processing tasks on network processor micro-engines involves complex tradeoff
    that relating to maximizing parallelism and pipelining. Due to an increase in the size of the code
    store and complexity of the application requirements, network ...

    Keywords: CPU scheduling, compiler optimizations, network processors, real-time scheduling

Results 1 - 20 of 351   Result page: 1   2   3   4   5   6   7   8   9   10   next   > >